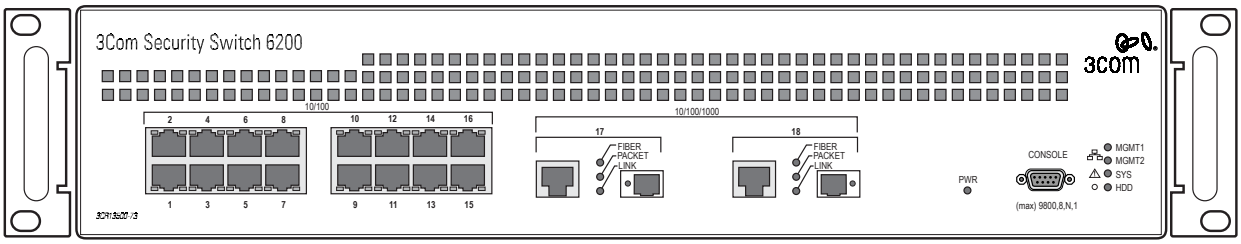
Security Switch 6200 Hardware and Software Users Guides



December 2003

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

Contents

4 Configuring the Security Switch 6200 System

5 Upgrading the System Software

6 Upgrading the System Software Using the Safe Upgrade and Rollback Features

7 Technical Support

A Technical Specifications

About this Guide

This guide describes how to install and configure the 3COM Security Switch 6200 hardware and system software. The Security Switch 6200 is based on the 3COM system software and may be referred to as the system.

Intended Audience

This guide is intended for system integrators and other qualified service personnel responsible for installing, configuring, and managing the system.

Conventions

The following conventions are used throughout this guide to emphasize certain information, such as, user input, screen options and output, and menu selections.

italics – Indicates book titles and user input variables.

`Courier` – Indicates user input and program output.

`Courier italics` – Indicates variables in commands.

Menu => – Indicates to select an Option from the menu pull-down.

Warnings, **Cautions**, and **Notes** indicate the following:

NOTES – Provide helpful suggestions or reference to materials not contained in this manual.

WARNING:
Warnings notify you to proceed carefully in order to avoid personal harm.

CAUTION:
Cautions notify you to proceed carefully in order to avoid damaging equipment or losing data.

Related Documentation

The following guides provide additional installation and configuration information for the system.

Security Switch 6200 Product Release Notes
Install Server Installation and Configuration Guide
Security Switch 6200 Applications Guide

Customer Support

To obtain technical tips or support, refer to the Technical Support chapter of this guide.

1 Introduction

The Security Switch 6200 is a high performance, turnkey security services switch that integrates best-in-class firewall, virtual private networks, intrusion detection, and content security engines. The system offers high port density, high availability, and simplicity of management in a compact, expandable form factor.

The system is a Network Processor-based security platform that provide exceptional performance while maintaining flexibility for security application support. The system's unique flow management and acceleration technology enables simultaneous processing of traffic by multiple services.

The system is used by medium to large enterprises to consolidate the functions of multiple appliances at a fraction of the cost.

This chapter describes the system components.

System Components

The system has a compact, expandable form factor and is either rack or table-top mountable. The system provides the following features:

- Fixed 16-10/100 Ethernet and 2-fiber or copper Gigabit Ethernet (GE) interfaces.
- Network Interface Module (NIM) powered by the Network Processor.
- Dual-processor motherboard (Application Module) with high-speed Pentium III processors.
- High-speed Ethernet backplane connecting the network and application processing modules.
- 40 GB hard drive.
- Two out-of-band 10/100 Ethernet management ports.
- Two USB ports (may be used for modem support).

- One serial console port.
- Two redundant, hot-swappable power supplies.
- Five expansion slots for optional VPN or other security acceleration cards.

Chassis

The chassis is front rack mountable, in a standard 19 inch rack.

Figure 1-1 displays the 6200 system's major components.

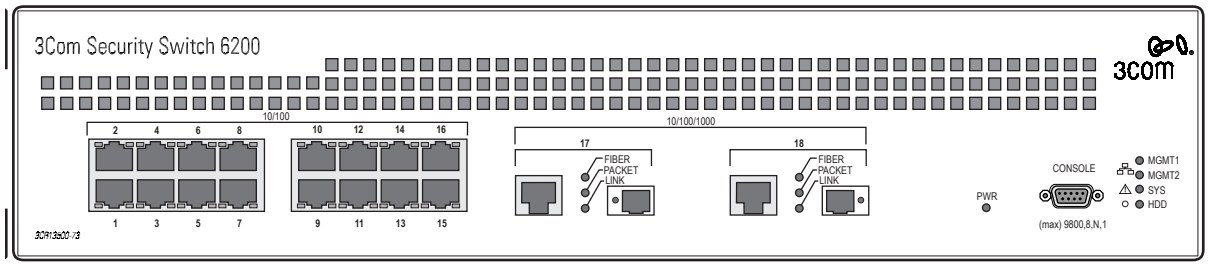


Figure 1-1 6200 Front View

Figure 1-2 displays the rear panel components.

NOTE: This figure is shown for reference only. The console connections should be made from the 6200 front panel, with the management connections taking place in the rear of the chassis.

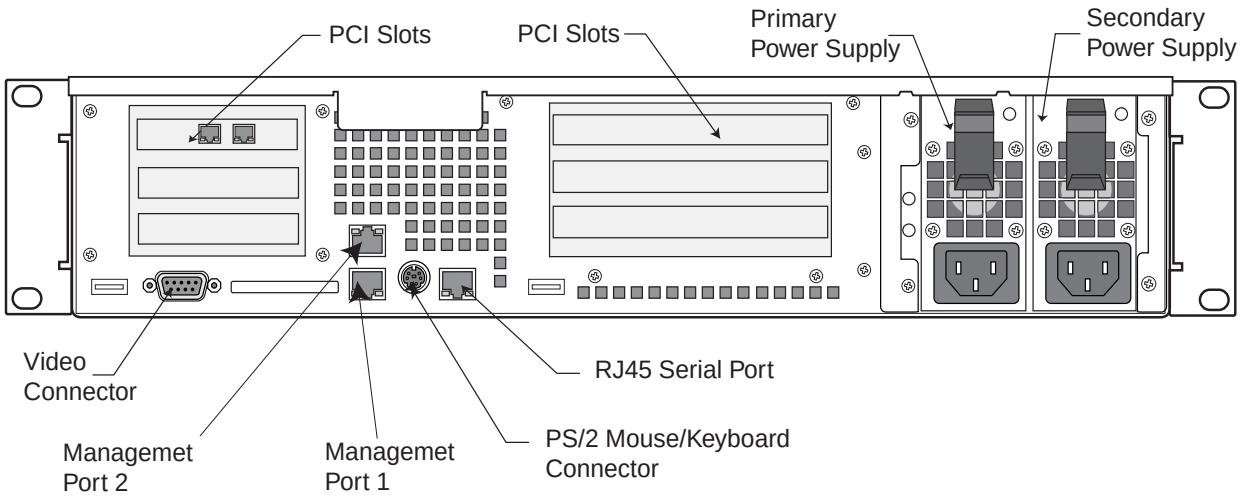


Figure 1-2 Rear Panel Component Layout

Management Options

The system provides two system management options:

- First time startup interview
- Configuration Tool

First Time Startup Interview

The system uses a built in, easy to configure, interview tool (cos_interview) that allows you to quickly configure your system for basic operations. For further information on the startup interview, refer to the *Interface Connections and First Time Start-Up* chapter of this guide.

Configuration Tool

The system uses a menu driven configuration interface (cos_config) for configuration purposes. This tool supports adding, modifying, or deleting any of the system configuration parameters. For further information on this tool, refer to the *Configuring the System* chapter of this guide.

2 Installation

This chapter describes the system installation, covering the following topics:

- Pre-installation considerations
- Chassis installation
- Interface connections

Before You Start

WARNING:
To ensure power connectivity, if you are using more than one power supply, be sure to use separate power sources.

Before installing your system, be sure that the site's environmental and space requirements allow optimal chassis access and operation. In addition, you need to verify that you have the equipment and the tools necessary to complete this installation.

Site Requirements

The system installation site should meet the following requirements:

Requirement	Description
Operating Temperature	0 to 40 degrees C
Relative Humidity	10% - 90%, non-condensing
Minimum Ventilation	6 inches (15.2 cm) to the front, back, and sides of the chassis
Service Clearance	30 inches (76.2 cm) at the front of the chassis
Power Sources	100 to 240 VAC outlets, with grounding and power surge protection
Rack	Standard 19-inch rack with grounding

Shipment Check

Using the packing slip as a reference, inspect package contents for missing or damaged items. If parts are missing or damaged, call your 3COM Systems Support Representative (Refer to Chapter 5, for contact information.). The following items, as a minimum, are included with your system:

- Chassis
- Mounting screws
- Rubber feet
- Two power cables
- One serial console port cable
- CDs containing the system software, product documentation, and applications
- Warranty card

Figure 2-1 shows the standard shipping contents:

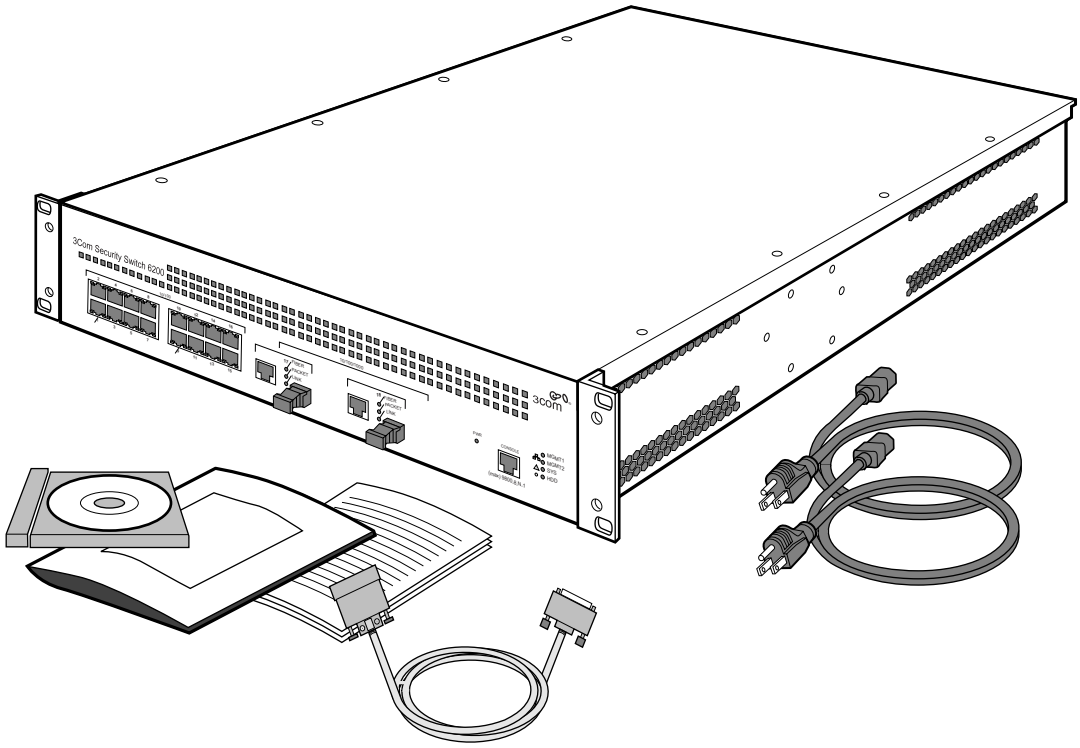


Figure 2-1 3COM Security Switch 6200 Shipping Contents

NOTE: 3COM recommends that you save the shipping containers in the event you need to send back one or more components.

Additional Equipment

- PC running RedHat Linux 6.2 or greater software. This software is used to support the Security Switch 6200 Graphical User Interface (GUI) and for hosting the Check Point™ FireWall-1® Management Server.
- PC running WinNT4/Win2K software. This software is used for launching the Check Point FireWall-1 GUI and the system's embedded WEB GUI.
- Security applications licenses to activate installed software on the system.

Required Equipment

To install the chassis in a standard rack you need certain hand tools, appropriate cabling, and additional hardware not included in the chassis shipment.

Tools

To install the chassis into a standard rack you need, as a minimum, a Phillips screwdriver (9" minimum, #2).

Cables

Cabling requirements are installation-specific. Prior to installation you should know:

- The kind and number of cables required for each type of interface.
- The distance limitations for each signal type. Table 2-1: provides the approximate cable distance limitations.

Table 2-1: Cable Distance Limitations

Cable Description	Distance Limitation
Craft port: RS-232 DB9 directly from the system	15 meters maximum (50 feet maximum)
Management Link port: 10/100	Cat 5 cable, 100 meters (328 feet)
Copper Ethernet Link Port: 10/100/1000	Cat 5 cable, 100 meters (328 feet)
Fiber Ethernet Link Port: Gigabit	62.5 micro-fiber - 275 meters (902 feet) 50 micro-fiber - 550 meters (1805 feet)

Table 2-2: shows the cables that ship with chassis.

Table 2-2: System Cables

Cable	Description
Power Cabling	Standard AC power cable.
Console Port	Serial shielded straight-through 9-pin D-sub female to 9-pin male cable.

Terminal or PC

A VT-100 terminal or a Personal Computer (PC) is required during installation. The terminal or PC is connected to the chassis's craft port, allowing you to monitor start-up diagnostics and to configure the unit for remote management access.

Chassis Rack Installation

The chassis can be installed in the front or center of a standard 19" rack.

Front Rack Mounting

To install the chassis in the front of your rack:

1. Remove the center brackets (one on each side) from the system.
2. Position the chassis in the rack by aligning the holes on its integrated front mounting brackets with the holes in the rack.
3. Insert the appropriate screws through the brackets and tighten. If the rack holes are not threaded, use cage-nuts over them. Figure 2-2 shows a chassis installation example.

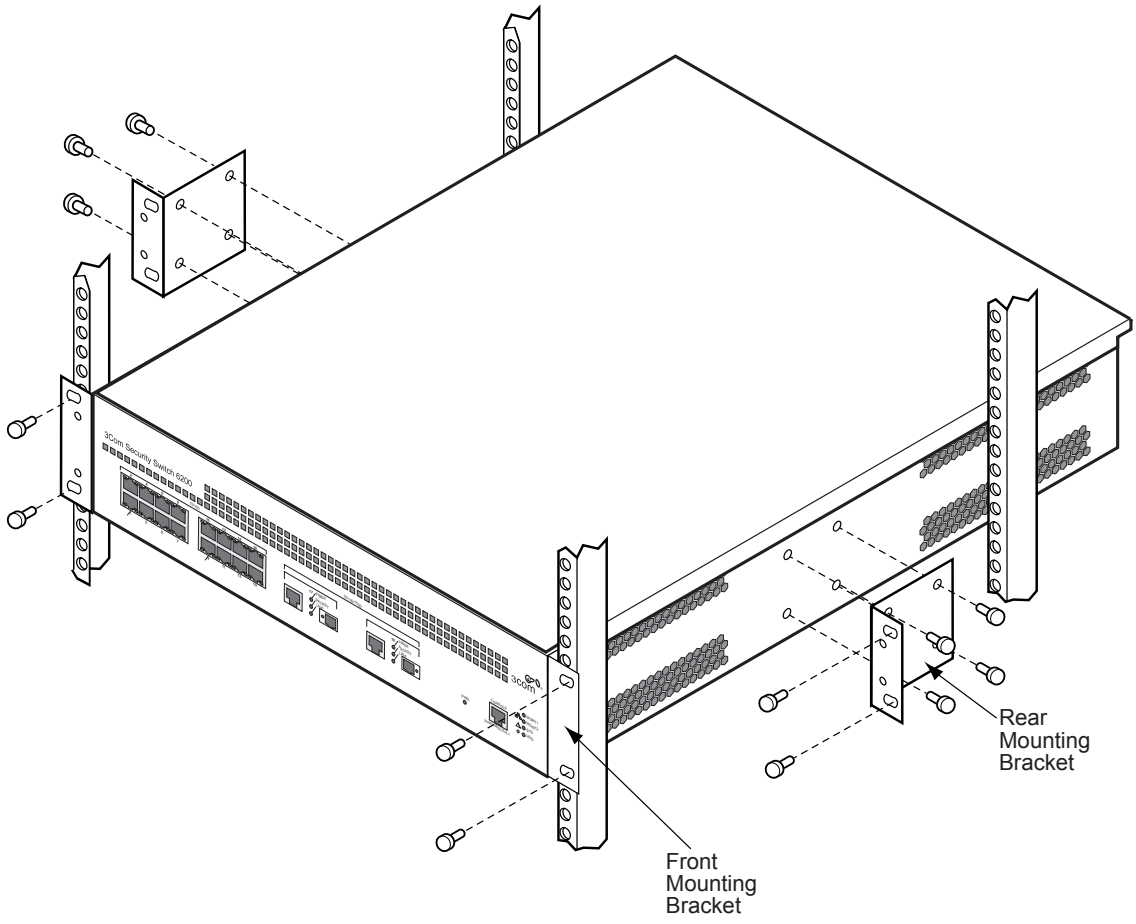
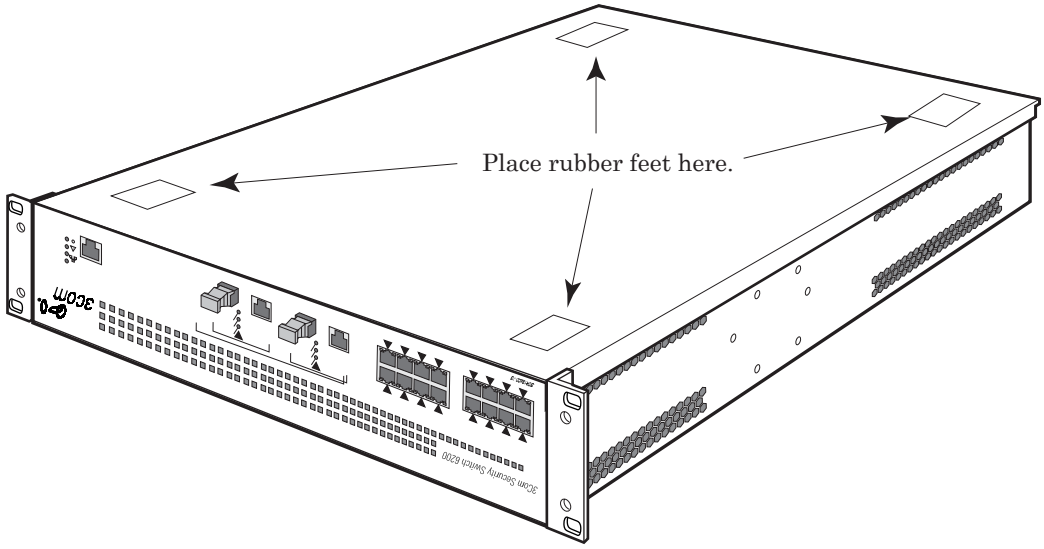


Figure 2-2 Front Rack Mounting the Chassis

Tabletop Mounting

The system can be mounted on any desk or table top. To do this you first need to attach the four rubber feet, supplied with the system, to the bottom of the box. To do this, complete the following:

1. Turn the system over onto its top with the bottom facing up.
2. Locate the indented feet locators, as shown in the following figure.



3. Peel backing off of the rubber feet and press them down firmly on the indents.

Once the rubber feet are installed you can mount the system on a solid flat surface.

3 Interface Connections and First Time Start-Up

This chapter describes the procedure for powering up the system for the first time. Specifically covered are the following:

- Connecting to the Management Console
- Powering Up the System
- First time configuration

Making Connections

This section describes connections to the chassis interfaces, including:

- Management serial port
- Ethernet port
- Power connections

Management Serial Port Connections

The system provides you with multiple ways to access the Management Console. You can connect to the console by either connecting a terminal or a PC to the system's serial (craft) connector or by Telneting into the system Management Console remotely.

For the initial configuration you can connect to the system through the craft port. Alternatively, you can connect to the system through telnet if you have the DHCP service in your network. By default, DHCP is enabled on your system, after your intital configuration you can disble the DHCP service.

To connect to the serial connector use the DB9 serial connector located on the front panel of the system.

NOTE: If you are connecting to the system Management Console using a terminal or PC, the serial port on the terminal or PC must be configured for 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control.

Connecting a Terminal or PC to the System Front Serial Craft Port

To connect a terminal or PC to the system front serial craft port:

1. Connect one end of a DB9-to-DB9 cable into the terminal or PC.
2. Connect the other end into the system serial craft port. Figure 3-1 shows the system connected to a laptop computer.

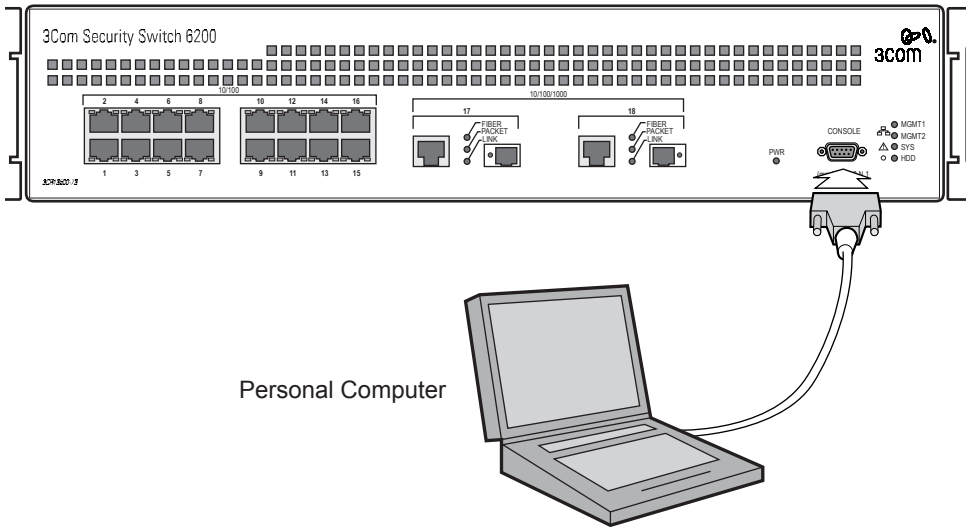


Figure 3-1 Connecting a Laptop Computer to the system Front Serial Craft Port

3. Set to VT-100 terminal emulation mode.

Connecting Remotely

To access the system remotely:

1. Connect one end of an RJ45-to-RJ45 cable into a remote access device.
2. Connect the other end into the Management port. Figure 3-2 shows the Management port module connected to a hub.

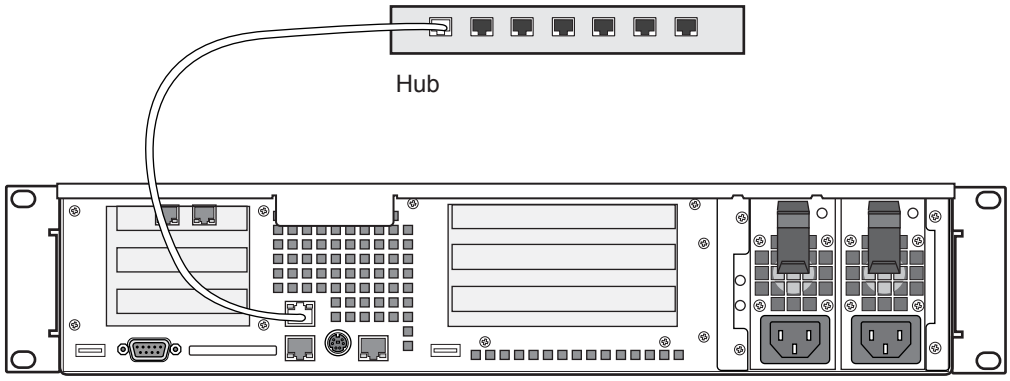


Figure 3-2 Connecting to the System Remotely

3. Telnet to configure IP.

Power Connections

CAUTION: To ensure power connectivity, if you are using more than one power supply, be sure to use separate power sources.

To connect power cabling:

1. Place the female end of the power cable into the power supply connector located on the back of the chassis. Refer to Figure 3-3 for the exact location.

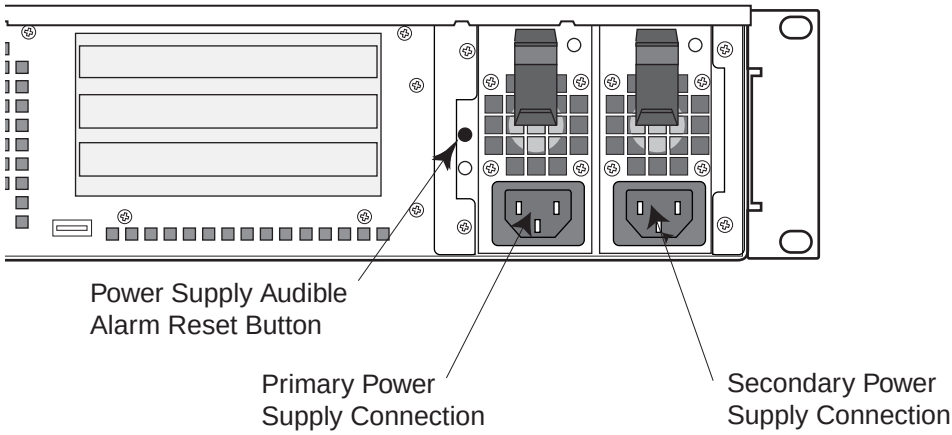


Figure 3-3 System Rear View Power Connections

NOTE: Before applying power to the system, be sure you have connected a terminal or PC to the craft port. This allows you enter commands needed at startup.

2. Attach the male end of the power cable into an AC power source. The system is powered up when power is applied to the power supplies.

NOTE: If the system is powered up with one power supply or if one of the power supplies experiences a loss of power, an audible alarm sounds. To silence this sound, press the red button located on the left side of the primary power supply.

Startup and Normal Operation LED Displays

During power up and normal operation, you can observe start-up activity by checking LED activity on the system front panel.

Table 3-1 describes the various front panel LEDs and their function.

Table 3-1 Front Panel LED Descriptions

LED	Color/Label	State	Description
10/100 Fast Ethernet	Green	On	Ethernet connectivity present.
	Yellow	Flashing	Traffic is present.
10/100/100 Fast Ethernet/Gigabit Ethernet	Fiber/Green	On	Fiber connectivity present.
	Activity/Green	Flashing	Traffic is present.
	Link/Green	On	Ethernet connectivity present.
Power/Sleep(PWR)	Green	On	Power on.
		Flashing [1]	In sleep state.
	Off	Off	Power is off.
MGMT1/MGMT2	Green	Random Flash	NIC activity present.
System Status (SYS)	Green	On	Running with normal operation.
		Flashing [2]	Degraded.
	Amber	On	Critical or non-recoverable condition.
		Flashing [2]	Non-critical condition.
	Off	Off	Post/system stop.
Disk Activity (HDD)	Green	Random Flash	Disk activity present.
	Off	Off [3]	No hard disk activity detected.

1. The PWR LED sleep indication is maintained on standby by the system. If the system is powered down without going through BIOS, the LED state in effect at the time of power off, is restored when the system is powered on until cleared by the BIOS. If the system is not powered down normally, the PWR LED may blink even though the SYS LED may be off due to a failure or configuration change that prevents the BIOS from running.
2. The Amber status takes precedence over the Green status. When the Amber LED is on or flashing, the Green LED is off.
3. This LED is also off when the system is powered off or in a sleep state.

POST Error Beep Codes

The following tables list POST error beep codes. Before system video initialization, the BIOS and BMC use these beep codes to inform users on error conditions.

BMC Generated POST Beep Codes

Code	Description
1-5-1-1	FRB failure (processor failure)
1-5-2-1	Empty Processor
1-5-2-2	No Processor
1-5-4-2	Power fault: DC power unexpectedly lost (power control failures)
1-5-4-3	Chipset control failure
1-5-4-4	Power control failure

BIOS Generated POST Error Beep Codes

Beeps	Error message	Description
1	Refresh timer failure	The memory refresh circuitry on the motherboard is faulty.
2	Parity error	Parity can not be reset.
3	Base memory failure	Base memory test failure. See Table 53. POST Memory Error 3-Beep Codes for additional error details.
4	System timer	System timer is not operational.
5	Processor failure	Processor failure detected.
6	Keyboard controller Gate A20 failure	The keyboard controller may be bad. The BIOS cannot switch to protected mode.
7	Processor exception interrupt error	The CPU generated an exception interrupt.
8	Display memory read/write error	The system video adapter is either missing or its memory is faulty. This is not a fatal error.
9	ROM checksum error	System BIOS ROM checksum error.
10	Shutdown register error	Shutdown CMOS register read/write error detected.
11	Invalid BIOS	General BIOS ROM error.

POST Memory Error 3-Beep Codes

Beep Code	Debug port 80h error Codes	Daignostic LED Decoder G=Green, R=Red, A=Amber				Meanings
		Hi			Low	
3	00h	Off	Off	Off	Off	No memory was found in the system
3	01h	Off	Off	Off	G	Memory mixed type detected.
3	02h	Off	Off	G	Off	EDO is not supported.
3	03h	Off	Off	G	G	First row memory test failure.
3	04h	Off	G	Off	Off	Mismatched DIMMs in a row.
3	05h	Off	G	Off	G	Base memory test failure.
3	06h	Off	G	G	Off	Failure on decompressing post module.
3	07h-odh	Off	G	G	G	Generic memory error.
		G	Off	Off	Off	
		G	Off	Off	G	
		G	Off	G	Off	
		G	Off	G	G	
		G	G	Off	Off	
		G	G	Off	G	
3	0Eh	G	G	G	Off	SMBUS protocol error.
3	0F-FFh	All other combinations.				Generic memory error.

First Time Startup

The system uses a built in, easy to configure, interview script that allows you to quickly configure your system for basic operations.

Once you have completed this interview, you can use the system Configuration Tool to set additional parameters.

The interview script is launched from the UNIX root prompt. To launch the interview script, complete the following.

NOTE: Within this interview, you can type the initial letter of an option and the press the Tab key to complete the entire string on supported choices. The Enter key is used to select default values.

1. Log into your system as root.

   NOTE: The password is admin.

2. Change to the bin directory within admin and list the files within this directory to locate the necessary interview file.

   ```
   [admin@xxxxx admin]# cd /usr/os/bin
   [admin@xxxxx bin]# ls
   ```

3. Locate the file cos_interview and execute the following command at the admin prompt:

   ```
   [admin@xxxxx bin]# ./cos_interview
   ```

Once the interview is launched, you are presented with an interactive interview. To begin your initial configuration, answer the following questions.

```
=======================================================
         Welcome to the Configuration Interview

This program is designed to guide you through the
configuration of your system by prompting you with a
series of questions.
=======================================================
```

1. Enter the Hostname.

   ```
   Hostname
   ========

   Enter the system hostname:
   ```

2. Enter the System time.

   ```
   System Time
   ===========

   The current date and time on this system is Mon Mar 10
   13:04:23 EST 2003

   Would you like to modify System time <Y or N>[N]: y
   ```

```
Please provide the date in "Mon DD YYYY" format, where
Mon : month in the form Jan, Feb, etc.
DD : day of month (1 - 31),
YYYY: for example 2002

Enter the Date :
```

3. Define the Time Zone.

```
Select a time zone based on the location of your system.

The current Time Zone is "present-time-zone"
Would you like to Modify the Time Zone <Y or N> [N]: y
Select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) Other (Enter GMT offset)
Enter choice <1 - 11>:

Select a country.
```

1)Antigua & Barbuda	18)Ecuador	35)Panama
2)Anguilla	19)Grenada	36)Peru
3)Netherlands Antilles	20)French Guiana	37)St Pierre & Miquelon
4)Argentina	21)Greenland	38)Puerto Rico
5)Aruba	22)Guadeloupe	39)Paraguay
6)Barbados	23)Guatemala	40)Suriname
7)Bolivia	24)Guyana	41)El Salvador
8)Brazil	25)Honduras	42)Turks & Caicos Is
9)Bahamas	26)Haiti	43)Trinidad & Tobago
10)Belize	27)Jamaica	44)United States
11)Canada	28)St Kitts & Nevis	45)Uruguay
12)Chile	29)Cayman Islands	46)St Vincent
13)Colombia	30)St Lucia	47)Venezuela
14)Costa Rica	31)Martinique	48)Virgin Islands (UK)
15)Cuba	32)Montserrat	49)Virgin Islands (US)
16)Dominica	33)Mexico	
17)Dominican Republic	34)Nicaragua	

```
Enter choice <1 - 49>:
```

4. Select a region.

```
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Standard Time - Indiana - most locations
6) Eastern Standard Time - Indiana - Crawford County
7) Eastern Standard Time - Indiana - Starke County
8) Eastern Standard Time - Indiana - Switzerland County
9) Central Time
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands

Enter choice <1 - 21>:
```

5. Define the Management Services.

```
Management Services
===================

Several methods are available for managing your system
through the 10/100 Ethernet interface on the host.
Select the desired management services.

Enable Telnet Server <disabled, enabled>[enabled]:
Enable FTP Server <disabled, enabled>[enabled]:

Add DNS Lookups <Y or N>[N]:

DNS Server IP Address [0.0.0.0]:
```

6. Configure the SNMP parameters.

```
Configure SNMP Network Management <Y or N>[N]:

Enabling SNMP ...

Enable SNMP Network Management <disabled, enabled>
[disabled]:
Enter SNMP Contact []:
Enter SNMP Location []:

The SNMP community string is the access string to
permit access to the SNMP protocol. A read-only "ro" or
read-write "rw" access may be specified. By default,
SNMP community string permits read-only access.
```

```
SNMP Communities
================

Community  Address    Netmask          Access
middle     10.1.1.22  255.255.255.255  read-write

Add the SNMP Communities <Y or N>[N]:
```

7. Configure the individual user accounts.

```
Accounts Configuration
======================

This section allows you to change your "root" password.
Additionally, you can set up accounts for users to log
into once the Interview is complete.

Set 'root' Password <Y or N>[Y]:

Additional user accounts can be defined, each with its
own username and password.

Add or Modify User Accounts <Y or N>[Y]:
Enter User Name []:
Enter password:
Verify password:
Enable Login Access <disabled, enabled>[disabled]:
Enter Access Level <Guest, Network Operator, Service
Operator, Administrator>[Guest]:
```

The following is an example display showing configured users.

```
User Accounts
=============

 User Name   Login Access    Access Level
 admin       enabled         Administrator
 foobar      enabled         Guest

Add or Modify User Accounts <Y or N>[Y]: n
```

8. Configure the host interfaces.

```
Host Interfaces
===============

This section will help you configure interfaces on the
Host. The system has two management ports, two GigaBit
Ethernet ports, and 16 10/100 ports.

NOTE: At least one management port must be configured
on the system.
```

```
Enter choice.

 1) fastethernet 1   12) fastethernet 12
 2) fastethernet 2   13) fastethernet 13
 3) fastethernet 3   14) fastethernet 14
 4) fastethernet 4   15) fastethernet 15
 5) fastethernet 5   16) fastethernet 16
 6) fastethernet 6   17) gigabitethernet 17
 7) fastethernet 7   18) gigabitethernet 18
 8) fastethernet 8   19) management 1
 9) fastethernet 9   20) management 2
 10) fastethernet 10 X) Exit
 11) fastethernet 11

Enter choice <1 - 20, X>[X]:

Enter IP Address [0.0.0.0/0]:
```

9. Configure all additional interfaces.

```
Continue configuring interfaces <Y or N>[N]:

Enter choice.

1) fastethernet 1
2) fastethernet 2
3) fastethernet 3
.
.
.
19) management 1
20) management 2
21) None

Enter choice <1 - 21>[1]:

Enter IP address and mask :

Continue configuring interfaces <Y or N>[N]:
```

Continue this step until all interfaces are configured.

10. Configure your default gateway.

```
Default gateway
===============

This section allows you to configure a default gateway
for the system. Please provide an IP address, in dotted
decimal format.

Default gateway [0.0.0.0]:
```

11. Configure NTP to achieve time synchronization.

```
Synchronizing the system's clock with an accurate
source is important for proper correlation of security
events. The system uses the Network Time Protocol (NTP)
to achieve time sychronization. The IP address of an
NTP server must be specified.

NTP Server
==========

Add NTP Server <Y or N>[Y]:
Enter NTP Server IP Address [0.0.0.0]:

=====================================================

Congratulations, you have finished the Interview.

To activate your interview settings, you MUST reboot
the system using the following command at the prompt:

# reboot
Exiting the Interview...
=====================================================
```

4 Configuring the Security Switch 6200 System

The system uses a menu driven configuration interface (cos_config) for configuration purposes. This tool supports adding, modifying, or deleting any of the system configuration parameters.

This configuration interface is launched from the UNIX admin prompt. To launch this tool, complete the following:

1. Log into your system as admin.

   ```
   username: admin
   password: admin
   ```

2. Change to the bin directory within admin and list the files within this directory to locate the necessary interview file.

   ```
   [admin@xxxxx admin]# cd /usr/os/bin
   [admin@xxxxx bin]# ls
   ```

3. Execute the file cos_config and execute the following command at the admin prompt:

   ```
   [admin@xxxxx bin]# ./cos_config
   ```

Once the configuration tool is launched, you are presented with an interactive main menu.

```
Configuration
=========
1) System Parameters
2) User Accounts
3) Network Time Protocol (NTP)
4) Domain Name Service (DNS)
5) Simple Network Management Protocol (SNMP)
6) Physical Interfaces
7) Tap Interfaces
8) Network Interfaces
9) IP Aliases
10) Static Routes
11) Static ARP Entries
12) Virtual Router Redundancy Protocol (VRRP)
X) Exit
```

To begin your configuration, select the desired option from the main menu.

NOTE: Within this configuration tool, you can type the initial letter of an option and the press the Tab key to complete the entire string on supported choices. The Enter key is used to select default values.

Configuring System Parameters

This section describes how to change your system settings. Specifically, how to:

- Change the system host name and domain name
- Change system information
- Change time information
- Enable external access ability

To configure system parameters:

1. Select Option 1 from the main menu.

   The present System Configuration is displayed. For example:

   ```
   System
   ======
   Host Name       helios
   Domain Name
   Date and Time   Mon Apr 07 15:28:27 EDT 2003
   Time Zone
   Telnet Server   enabled
   FTP Server      enabled
   WEB Timeout     20
   Default Gateway 192.168.10.1

   Would You Like to Modify the System Parameters <Y or
   N>[N]:
   ```

2. To change any of the system parameters enter y, or press the Return key to leave system parameters unchanged.

```
Enter the System Host Name [hostname]:
Enter the System Domain Name []:
Enter the Time [15:28:40]:
Enter the Date [Apr 07 2003]:
Would You Like to Modify the Time Zone <Y or N>[N]:
```

3. To change the time zone enter y or press the Return key to leave system parameters unchanged.

```
Select a time zone based on the location of your system.

Select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) Other (Enter GMT offset)
Enter choice <1 - 11>:

Select a country.

1)Antigua & Barbuda     18)Ecuador          35)Panama
2)Anguilla              19)Grenada          36)Peru
3)Netherlands Antilles  20)French Guiana    37)St Pierre & Miquelon
4)Argentina             21)Greenland        38)Puerto Rico
5)Aruba                 22)Guadeloupe       39)Paraguay
6)Barbados              23)Guatemala        40)Suriname
7)Bolivia               24)Guyana           41)El Salvador
8)Brazil                25)Honduras         42)Turks & Caicos Is
9)Bahamas               26)Haiti            43)Trinidad & Tobago
10)Belize               27)Jamaica          44)United States
11)Canada               28)St Kitts & Nevis 45)Uruguay
12)Chile                29)Cayman Islands   46)St Vincent
13)Colombia             30)St Lucia         47)Venezuela
14)Costa Rica           31)Martinique       48)Virgin Islands (UK)
15)Cuba                 32)Montserrat       49)Virgin Islands (US)
16)Dominica             33)Mexico
17)Dominican Republic   34)Nicaragua

Enter choice <1 - 49>:
```

4. Select a region.

```
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Standard Time - Indiana - most locations
6) Eastern Standard Time - Indiana - Crawford County
7) Eastern Standard Time - Indiana - Starke County
8) Eastern Standard Time - Indiana - Switzerland County
9) Central Time
10) Central Time - Michigan - Wisconsin border
11) Central Time - North Dakota - Oliver County
12) Mountain Time
13) Mountain Time - south Idaho & east Oregon
14) Mountain Time - Navajo
15) Mountain Standard Time - Arizona
16) Pacific Time
17) Alaska Time
18) Alaska Time - Alaska panhandle
19) Alaska Time - Alaska panhandle neck
20) Alaska Time - west Alaska
21) Aleutian Islands

Enter choice <1 - 21>:
```

5. Define the Management Services.

```
Enable Telnet Server <disabled, enabled>[enabled]:
Enable FTP Server <disabled, enabled>[enabled]:
Enter WEB Timeout [20]:
Enter Default Gateway [0.0.0.0]:
```

6. Select option 1 from the main menu to display your changed system parameters. For example:

```
Enter choice <1 - 12, X>[X]: 1

System
======
Host Name       helios
Domain Name     3com.com
Date and Time   Mon Apr 07 15:29:03 EDT 2003
Time Zone       America/New_York
Telnet Server   enabled
FTP Server      enabled
WEB Timeout     20
Default Gateway 192.168.10.1

Would You Like to Modify the System Parameters <Y or
N>[N]:
```

7. Enter y to make further changes or press the Enter key to return to the main menu.

Configuring User Accounts

Each system user is defined by the user's name, password, and access level. Collectively, these properties define each user's profile. Login access allows you to login into the unix shell, setting this to disabled allows you to only have WEB access. To configure individual user accounts:

1. Select Option 2 from the main menu.

```
Accounts Configuration
======================
Additional user accounts can be defined, each with
there own username and password.

User Accounts
=============

 User Name     Login Access       Access Level
 admin         enabled            Administrator


Modify the User Accounts <Add, Delete, Modify or
eXit>[eXit]:
```

2. Enter the desired option and make changes as necessary or enter X to return to the main menu. The following is an example of a user being added:

```
Modify the User Accounts <Add, Delete, Modify or
eXit>[eXit]: a

Enter User Name []: fred
Enter password:
Verify password:
Enable Login Access <disabled, enabled>[disabled]:
enabled
Enter Access Level <Guest, Network Operator, Service
Operator, Administrator>[Guest]: administrator

User Accounts
=============

 User Name     Login Access       Access Level
 admin         enabled            Administrator
 fred          enabled            Administrator
```

3. Enter the desired option and make more changes or enter X to return to the main menu.

```
Modify the User Accounts <Add, Delete, Modify or
eXit>[eXit]:
```

Configuring the Network Time Protocol (NTP)

The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. It provides accuracies typically within a millisecond on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time (UTC) through a Global Positioning Service (GPS) receiver, for example. Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability.

To configure NTP:

1. Select Option 3 from the main menu.

```
NTP Servers
===========
xxx.xxx.xx.x

Modify the NTP Servers <Add, Delete or eXit>[eXit]:
```

2. Enter the desired option and add or delete an NTP server or enter X to return to the main menu.

Configuring Domain Name Resolution

Domain name resolution allows you translate and search domain names. The Domain Name System (DNS) is a global network of servers that translate host names like www.mycompany.com into numerical IP (Internet Protocol) addresses, for example 24.62.13.19.

To configure domain name resolution:

1. Select Option 4 from the main menu.

```
Domain Name Resolution Configuration
====================================
1) DNS Servers
2) DNS Search Domains
X) Exit

Enter choice <1 - 2, X>[X]: 1
```

2. Enter the desired option. For example:

```
Enter choice <1 - 2, X>[X]: 1

DNS Servers
===========
Modify the DNS Server List <Add, Delete or eXit>[eXit]: a

DNS Server's IP Address [0.0.0.0]: 10.1.1.50

DNS Servers
===========
10.1.1.50

Modify the DNS Server List <Add, Delete or eXit>[eXit]:

Domain Name Resolution Configuration
====================================
1) DNS Servers
```

```
2) DNS Search Domains
X) Exit

Enter choice <1 - 2, X>[X]: 2

DNS Search Domains
==================

Modify the DNS Domain Search List <Add, Delete or
eXit>[eXit]: a

Enter DNS Search Domain []: 3com.com

DNS Search Domains
==================
3com.com

Modify the DNS Domain Search List <Add, Delete or
eXit>[eXit]:

Domain Name Resolution Configuration
====================================
1) DNS Servers
2) DNS Search Domains
X) Exit

Enter choice <1 - 2, X>[X]:
```

3. Enter the desired option or enter X to return to the main menu.

Configuring the Simple Network Management Protocol (SNMP)

To configure SNMP:

1. Select Option 5 from the main menu.

```
SNMP configuration
==================
1) SNMP Server
2) Communities
3) Trap Destinations
X) Exit
```

2. Configure SNMP Servers. For example:

```
Enter choice <1 - 3, X>[X]: 1

SNMP Server
===========
Enabled    enabled
Contact    Root <root@localhost> (configure /etc/snmp/
snmp.local.conf)

Location   Unknown (edit /etc/snmp/snmpd.conf)

Would You Like to Modify the SNMP Configuration <Y or
N>[N]: y

Enable SNMP Network Management <disabled,
enabled>[enabled]:
Enter SNMP Contact [Root <root@localhost> (configure /
```

```
etc/snmp/snmp.local.conf)]: srhen@crossbeamsys.com
Enter SNMP Location [Unknown (edit /etc/snmp/
snmpd.conf)]: Lab

SNMP configuration
==================
1) SNMP Server
2) Communities
3) Trap Destinations
X) Exit

Enter choice <1 - 3, X>[X]: 1

SNMP Server
===========
Enabled    enabled
Contact    lab@3com.com
Location   The Lab

Would You Like to Modify the SNMP Configuration <y or
n>[n]:
```

3. Enter y to modify the SNMP configuration or n to return to the SNMP Configuration menu.

```
SNMP configuration
==================

1) SNMP Server
2) Communities
3) Trap Destinations
X) Exit
```

4. Configure SNMP Communities. For example:

```
Enter choice <1 - 3, X>[X]: 2

SNMP Communities
================

 Community      Address        Netmask      Access


Change the SNMP Communities <Add, Delete or
eXit>[eXit]: a
Enter Community Name []: foobar
Enter IP Source Addresses [0.0.0.0/32]: 10.2.1.48/32
Enter Access Mode <read-only, read-write>[read-only]:
read-write
```

```
SNMP Communities
================

Community    Address      Netmask          Access
foobar       10.2.1.48    255.255.255.255  read-write

Change the SNMP Communities <Add, Delete or
eXit>[eXit]: a

Enter Community Name []: public
Enter IP Source Addresses [0.0.0.0/32]: 10.0.0.0/8
Enter Access Mode <read-only, read-write>[read-only]:

SNMP Communities
================

Community    Address      Netmask          Access
foobar       10.2.1.48    255.255.255.255  read-write
public       10.0.0.0     255.0.0.0        read-only

Change the SNMP Communities <Add, Delete or
eXit>[eXit]:
```

5. Enter the desired option or enter X to return to SNMP Configuration Menu.

```
SNMP configuration
==================

1) SNMP Server
2) Communities
3) Trap Destinations
X) Exit
```

6. Configure SNMP Trap Destinations. For example:

```
Enter choice <1 - 3, X>[X]: 3

SNMP Traps
==========

Destination   Port     Type         Version   Community


Change the SNMP Trap Destinations <Add, Delete, Modify
or eXit>[eXit]: a
Enter Trap Destination [0.0.0.0]: 10.2.1.48
Enter Port Number [162]:
Enter Trap Type <trap, inform>[trap]:
Enter SNMP Version <SNMPv1, SNMPv2c, SNMPv3>[SNMPv1]:
Enter Community []: foobar
```

```
SNMP Traps
==========

 Destination   Port      Type     Version    Community
 10.2.1.48     162       trap     SNMPv1     foobar

Change the SNMP Trap Destinations <Add, Delete, Modify
or eXit>[eXit]:
```

7. Enter the desired option or enter X to return to SNMP Configuration Menu.

```
SNMP configuration
==================

1) SNMP Server
2) Communities
3) Trap Destinations
X) Exit
```

8. Enter the desired option or enter X to return to the main menu.

Configuring Physical Interfaces

There are three types of physical interfaces on the system: management, gigabitethernet, and fastethernet. The management interfaces allow you to manage the configured interfaces.

To configure the physical interfaces:

1. Select Option 6 from the main menu.

```
Physical Interfaces
===================

                   MAC Address
Interface          (Configured)           Auto  Duplex  Speed
                                          neg
management 1        00:03:47:f1:aa:52 (N) on    half    10
management 2        00:03:47:f1:aa:53 (N) on    half    10
fastethernet 1                        (N) on    half    10
fastethernet 2                        (N) on    half    10
fastethernet 3                        (N) on    half    10
fastethernet 4                        (N) on    half    10
fastethernet 5                        (N) on    half    10
fastethernet 6                        (N) on    half    10
fastethernet 7                        (N) on    half    10
fastethernet 8                        (N) on    half    10
fastethernet 9                        (N) on    half    10
fastethernet 10                       (N) on    half    10
fastethernet 11                       (N) on    half    10
fastethernet 12                       (N) on    half    10
fastethernet 13                       (N) on    half    10
```

```
                    MAC Address
Interface           (Configured)           Auto  Duplex  Speed
                                           neg
fastethernet 14                      (N) on    half    10
fastethernet 15                      (N) on    half    10
fastethernet 16                      (N) on    half    10
gigabitethernet 17                   (N) on    half    10
gigabitethernet 18                   (N) on    half    10

Modify Physical Interface Parameters <y or n>[n]:
```

2. Enter y to modify a physical interface or n to return to the main menu. For example:

```
Modify Physical Interface Parameters <y or n>[n]: y
Enter the Interface Name [fastethernet 1]:
MAC Address []: 00:00:a2:00:00:01
Auto Negotiate <off, on>[on]: off
Duplex <half, full>[half]: full
Speed <10, 100, 1000, unknown>[10]:

Physical Interfaces
===================

                    MAC Address
Interface           (Configured)           Auto  Duplex  Speed
                                           neg
management 1         00:03:47:f1:aa:52 (N) on    half    10
management 2         00:03:47:f1:aa:53 (N) on    half    10
fastethernet 1       00:00:a2:00:00:01 (Y) off   full    10
fastethernet 2                         (N) on    half    10
fastethernet 3                         (N) on    half    10
fastethernet 4                         (N) on    half    10
fastethernet 5                         (N) on    half    10
fastethernet 6                         (N) on    half    10
fastethernet 7                         (N) on    half    10
fastethernet 8                         (N) on    half    10
fastethernet 9                         (N) on    half    10
fastethernet 10                        (N) on    half    10
fastethernet 11                        (N) on    half    10
fastethernet 12                        (N) on    half    10
fastethernet 13                        (N) on    half    10
fastethernet 14                        (N) on    half    10
fastethernet 15                        (N) on    half    10
fastethernet 16                        (N) on    half    10
gigabitethernet 17                     (N) on    half    10
```

```
                    MAC Address
Interface           (Configured)          Auto  Duplex  Speed
                                          neg
gigabitethernet 18                   (N) on    half    10

Modify Physical Interface Parameters <Y or N>[N]:
```

3. Enter y to modify additional physical interfaces or n to return to the main menu.

Configuring Tap Interfaces

Tap interfaces are used to copy the input and output packets from a physical interface prior to the processing by the firewall acceleration process. These taps can be used by intrusion detection software to sniff the interface. Tap interfaces can be given any device name of up to 15 characters, and a single tap can capture the traffic for multiple physical interfaces. To configure Tap Interfaces:

1. Select Option 7 from the main menu.

```
Tap Interfaces
=============

Name       Physical Interfaces

Modify the Tap Interfaces <Add, Delete, Modify or
eXit>[eXit]: a
```

2. Enter the desired option to add, delete, or modify a tap interface or enter x to return to the main menu. For example:

```
Tap Name []: tap1
Physical Interfaces []: fastethernet 1, fastethernet 2,
gigabitethernet 17

Tap Interfaces
=============
Name  Physical Interfaces
tap1  fastethernet 1, fastethernet 2, gigabitethernet 17

Modify the Tap Interfaces <Add, Delete, Modify or
eXit>[eXit]:
```

3. Enter the desired option to add, delete, or modify additional tap interfaces or enter x to return to the main menu. For example:

```
Tap Name []: tap2
Physical Interfaces []: fastethernet 3

Tap Interfaces
=============
Name   Physical Interfaces
tap1   fastethernet 1, fastethernet 2, gigabitethernet 17
tap2   fastethernet 3
```

Configuring Network Interfaces

A network interface associates an IP address with a physical connection and optionally a VLAN id. To configure network interfaces:

1. Select Option 8 from the main menu.

```
IP Interfaces
=============

Enabled      Address       Netmask        Broadcast      MTU
management 1 192.168.10.6  255.255.255.0  192.168.10.255 1500
enabled
```

2. To add a network interface, select add from the main menu. For example:

```
Modify the IP Interfaces <Add, Delete, Modify or
eXit>[eXit]: a
Physical Interface [fastethernet 1]:
VLAN Interface <Y or N>[N]:
Interface State <disabled, enabled>[enabled]:
Enter the IP Address [0.0.0.0/0]: 128.205.1.23/24
Broadcast Address [128.205.1.255]:
MTU [1500]:

IP Interfaces
=============

Enabled         Address      Netmask       Broadcast     MTU
management 1    192.168.10.6 255.255.255.0 192.168.10.25 1500
enabled                                    5
fastethernet 1 128.205.1.23 255.255.255.0 128.205.1.255 1500
enabled
```

3. Enter the desired option to add, delete, or modify additional network interfaces or enter x to return to the main menu. For example:

```
Modify the IP Interfaces <Add, Delete, Modify or
eXit>[eXit]: a
Physical Interface [fastethernet 1]:
VLAN Interface <Y or N>[N]: y Enter VLAN ID <1 - 4095>:
100
Interface State <disabled, enabled>[enabled]:
Enter the IP Address [0.0.0.0/0]: 128.205.2.23/24
Broadcast Address [128.205.2.255]:
MTU [1500]:
```

```
IP Interfaces
=============

 Enabled        Address      Netmask       Broadcast      MTU
 management 1  192.168.10.6 255.255.255.0 192.168.10.25  1500
 enabled                                  5
 fastethernet  128.205.1.23 255.255.255.0 128.205.1.255  1500
 1 enabled
 fastethernet  vlan 100     255.255.255.0 128.205.2.255  1500
 1 enabled     128.205.2.23


Modify the IP Interfaces <Add, Delete, Modify or
eXit>[eXit]:
```

4. Enter the desired option to add, delete, or modify additional network interfaces or enter x to return to the main menu.

Configuring IP Aliases

IP aliases are additional network addresses that are assigned to a network interface. To configure IP Aliases:

1. Select Option 9 from the main menu.

```
IP Aliases
==========

 Interface      IP Address      Netmask     Broadcast


Modify the IP Aliases <Add, Delete, Modify or
eXit>[eXit]: a
```

2. Enter the desired option to add, delete, or modify an IP alias or enter x to return to the main menu. For example:

```
Enter Interface [fastethernet 1]:
VLAN Interface <Y or N>[N]:
Enter IP Address [0.0.0.0]: 128.205.1.24
Enter Network Mask [255.255.0.0]: 255.255.0.0
Enter Broadcast Address [128.205.255.255]:

IP Aliases
==========

Interface      IP Address    Netmask      Broadcast
fastethernet 1 128.205.1.24  255.255.0.0  128.205.255.255

Modify the IP Aliases <Add, Delete, Modify or
eXit>[eXit]: m
Enter Interface [fastethernet 1]:
VLAN Interface <Y or N>[N]:
Enter IP Address [0.0.0.0]: 128.205.1.24
Enter Network Mask [255.255.0.0]: 255.255.255.0
Enter Broadcast Address [128.205.1.255]:
```

```
    IP Aliases
    ==========

Interface      IP Address    Netmask      Broadcast
fastethernet 1 128.205.1.24  255.255.0.0  128.205.255.255
fastethernet 1 128.205.1.24  255.255.0.0  128.205.1.255

    Modify the IP Aliases <Add, Delete, Modify or
    eXit>[eXit]: a
    Enter Interface [fastethernet 1]:
    VLAN Interface <Y or N>[N]: y
    Enter VLAN ID <1 - 4095>: 100
    Enter IP Address [0.0.0.0]: 128.205.2.24
    Enter Network Mask [255.255.0.0]: 255.255.255.0
    Enter Broadcast Address [128.205.2.255]:

    IP Aliases
    ==========

Interface      IP Address    Netmask      Broadcast
fastethernet 1 128.205.1.24  255.255.0.0  128.205.255.255
fastethernet 1 128.205.1.24  255.255.0.0  128.205.1.255
fastethernet 1 128.205.2.24  255.255.0.0  128.205.2.255
vlan 100

    Modify the IP Aliases <Add, Delete, Modify or
    eXit>[eXit]:
```

3. Enter the desired option to add, delete, or modify additional IP aliases or enter x to return to the main menu.

Configuring Static Routes

Static IP routes are user-defined routes that cause packets moving between a source and a destination to take a specific path.

To configure Static Routes:

1. Select Option 10 from the main menu.

```
Static Routes
=============

 Destination   Netmask        Gateway           Metric
```

2. Enter the desired option to add, delete, or modify a static route or enter x to return to the main menu. For example:

```
Modify the Static Routes <Add, Delete, Modify or
eXit>[eXit]: a
Enter Destination [0.0.0.0/0]: 10.0.0.0
Enter Network Mask in dot notation [0.0.0.0]: 255.0.0.0
Enter the Next Hop Gateway [0.0.0.0]: 192.168.10.1
Enter the Metric [1]:
```

```
Static Routes
=============

Destination   Netmask        Gateway           Metric
10.0.0.0      255.0.0.0      192.168.10.1      1
```

```
Modify the Static Routes <Add, Delete, Modify or
eXit>[eXit]: a
Enter Destination [0.0.0.0/0]: 192.168.20.0/24
Enter the Next Hop Gateway [0.0.0.0]: 192.168.10.1
Enter the Metric [1]: 2
```

```
Static Routes
=============

Destination   Netmask        Gateway           Metric
10.0.0.0      255.0.0.0      192.168.10.1      1
192.168.20.0  255.255.255.0  192.168.10.1      2
```

```
Modify the Static Routes <Add, Delete, Modify or
eXit>[eXit]:
```

3. Enter the desired option to add, delete, or modify additional static routes or enter x to return to the main menu.

Configuring Static ARP Entries

You define static Address Resolution Protocol (ARP) entries by relating an IP address to a MAC address.

To configure static ARP entries:

1. Select Option 11 from the main menu.

```
Static ARP Entries
==================
IP Address       MAC Address
```

2. Enter the desired option to add, delete, or modify a static ARP entry or enter x to return to the main menu. For example:

```
Modify the Static Hosts <Add, Delete, Modify or
eXit>[eXit]: a
Enter Host IP Address [0.0.0.0]: 128.205.1.30
Enter MAC Address []: 00:00:a2:00:00:02

Static ARP Entries
==================
IP Address       MAC Address
128.205.1.30     00:00:a2:00:00:02

Modify the Static Hosts <Add, Delete, Modify or
eXit>[eXit]: a
Enter Host IP Address [0.0.0.0]: 128.205.1.31
Enter MAC Address []: 00:00:a2:00:00:03

Static ARP Entries
==================
IP Address       MAC Address
128.205.1.30     00:00:a2:00:00:02
128.205.1.31     00:00:a2:00:00:03

Modify the Static Hosts <Add, Delete, Modify or
eXit>[eXit]:
```

3. Enter the desired option to add, delete, or modify additional static ARP entries or enter x to return to the main menu.

Configuring the Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy Protocol (VRRP) dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. The system can be configured to run the VRRP protocol in conjunction with one or more other systems attached to a LAN.

VRRP which manages automatic switchover from one VPN Concentrator to another in a redundant installation. Automatic switchover provides user access to the VPN even if one VPN is out of service for some reason, for example a system crash, power failure, hardware failure, physical interface failure, system shutdown or reboot.

These functions apply only to installations where two or more VPNs are in parallel, with the Public interfaces of all systems on a common LAN and with the Private and/or External interfaces of all systems on different common LANs. One VPN is the Master system, and the others are Backup systems. A Backup system acts as a virtual Master system when a switchover occurs. VRRP works only on LAN (Ethernet) interfaces, not on WAN interfaces.

To configure VRRP:

1. Select Option 12 from the main menu.

```
VRRP Configuration
==================

Virtual Router Redundancy Protocol can be defined, each
with its own identifier.
```

```
VRRP Configurations
===================

VRRP ID                          : 1
Enabled                          : disabled
VRRP Interface                   : fastethernet 1
Enable VRRP MAC                  : disabled
Preemption                       : disabled
Priority                         : 100
Advertisement Interval (seconds) : 1
Group ID                         : 1
IP Addresses                     : 30.0.0.10
```

2. Enter the desired option to add, delete, or modify a VRRP entry or enter x to return to the main menu. For example:

```
Modify the VRRP Configuration <Add, Delete, Modify or
eXit>[eXit]: m
Enter VRRP ID [0]: 1
Enable <disabled, enabled>[disabled]: enabled
Enter Interface [fastethernet 1]:
VLAN Interface <Y or N>[N]:
Enable VRRP MAC <disabled, enabled>[disabled]:
Enable Preemption <disabled, enabled>[disabled]:
Enter Priority [100]:
Enter Advertisement Interval (seconds) [1]:
Enter Group ID [1]:
Enter IP Addresses Separated by Comma [30.0.0.10]:

VRRP Configurations
===================

VRRP ID                          : 1
Enabled                          : enabled
VRRP Interface                   : fastethernet 1
Enable VRRP MAC                  : disabled
Preemption                       : disabled
Priority                         : 100
Advertisement Interval (seconds) : 1
Group ID                         : 1
IP Addresses                     : 30.0.0.10

Modify the VRRP Configuration <Add, Delete, Modify or
eXit>[eXit]: a
```

```
Enter VRRP ID [0]: 2
Enable <disabled, enabled>[disabled]:
Enter Interface [management 0]: fastethernet 1
VLAN Interface <Y or N>[N]: y
Enter VLAN ID <1 - 4095>: 100
Enable VRRP MAC <disabled, enabled>[disabled]: enabled
Enable Preemption <disabled, enabled>[disabled]:
Enter Priority [0]: 100
Enter Advertisement Interval (seconds) [1]:
Enter Group ID [0]: 1
Enter IP Addresses Separated by Comma []: 30.0.0.10

VRRP Configurations
===================

VRRP ID                           : 1
Enabled                           : enabled
VRRP Interface                    : fastethernet 1
Enable VRRP MAC                   : disabled
Preemption                        : disabled
Priority                          : 100
Advertisement Interval (seconds)  : 1
Group ID                          : 1
IP Addresses                      : 30.0.0.10

VRRP ID                           : 2
Enabled                           : disabled
VRRP Interface                    : fastethernet 1
                                  vlan 100
Enable VRRP MAC                   : enabled
Preemption                        : disabled
Priority                          : 100
Advertisement Interval (seconds)  : 1
Group ID                          : 1
IP Addresses                      : 30.0.0.10
```

Exiting from the Configuration Tool

To exit from the system Configure Tool, select Option X from the main menu.

```
Enter choice <1 - 12, X>[X]: X
```

Saving Your System Configuration

To save your configuration, at the admin prompt, use the following command:

```
[admin@xxxxx bin]# ./cos_show_system -f /directory/filename
```

Where the directory specifies the directory where the file is located, and the filename is the actual configuration file. The following is an example of this command:

```
[admin@helios bin]$ ./cos_show_system -f /tmp/foo
```

Restoring Your System Configuration

To restore your configuration to its previous configuration, at the admin prompt, use the following command:

```
[admin@xxxxx bin]# ./cos_set_system -f /directory/filename
```

Where the directory specifies the directory where the file is located, and the filename is the actual configuration file. The following is an example of this command:

```
[admin@helios bin]$ ./cos_set_system -f /tmp/foo
```

Displaying Your System Configuration

To display a configuration, at the admin prompt, use the following command:

```
[admin@xxxxx bin]# ./cos_show_system
```

The following is an example of this command:

```
[admin@helios bin]$ ./cos_show_system

<system>

<data
hostname="helios"
domainname="3com.com"
timezone="America/New_York"
telnet_server="enabled"
ftp_server="enabled"
gateway="192.168.10.1"
</data>
</system>

<ntp_server>
<data
address="127.127.1.0"
></data>

</ntp_server>
<dns_server>
<data
```

```
address="10.1.1.50"
></data>
</dns_server>

<dns_search>
<data
domainname="3com.com"
></data>
</dns_search>

<snmp_server>
<data
enable="enabled"
contact="lab@3com.com"
location="The Lab"
></data>
</snmp_server>

<snmp_community>
<data
community="foobar"
address="10.2.1.48"
access="read-write"
></data>
<data
community="public"
address="10.0.0.0"
mask="255.0.0.0"
></data>

</snmp_community>
<snmp_trap_destination>
<data
host="10.2.1.48"
community="foobar"
></data>
</snmp_trap_destination>

<physical_interface>
<data
ifname="fastethernet 1"
mac_addr="00:00:a2:00:00:01"
autoneg="off"
duplex="full"
speed="10"
></data>
<data
ifname="fastethernet 15"
autoneg="off"
duplex="half"
speed="100"
></data>
</physical_interface>
```

```
<ip_interface>
<data
ifname="management 1"
address="192.168.10.6"
></data>
<data
ifname="fastethernet 1"
address="128.205.1.23"
mask="255.255.255.0"
></data>
<data
ifname="fastethernet 1"
vlan="100"
address="128.205.2.23"
mask="255.255.255.0"
></data>
</ip_interface>

<ip_alias>
<data
ifname="fastethernet 1"
address="128.205.1.24"
mask="255.255.255.0"
></data>
<data
ifname="fastethernet 1"
vlan="100"
address="128.205.2.24"
mask="255.255.255.0"
></data>
</ip_alias>

<static_route>
<data
destination="10.0.0.0"
mask="255.0.0.0"
gateway="192.168.10.1"
></data>
<data
destination="192.168.20.0"
mask="255.255.255.0"
gateway="192.168.10.1"
metric="2"
></data>
</static_route>

<static_host>
<data
ip_addr="128.205.1.30"
mac_addr="00:00:a2:00:00:02"
></data>
<data
```

```
ip_addr="128.205.1.31"
mac_addr="00:00:a2:00:00:03"
></data>
</static_host>

<account>
<data
username="admin"
shell="enabled"
access_level="Administrator"
></data>
<data
username="foobar"
shell="enabled"
></data>
<data
username="fred"
shell="enabled"
access_level="Administrator"
></data>
</account>

<tap_interface>
<data
tapname="tap1"
ifnames="fastethernet 1, fastethernet 2,
gigabitethernet 17"
></data>
<data
tapname="tap2"
ifnames="fastethernet 3"
></data>
</tap_interface>

<vrrp>
<data
enabled="enabled"
name="fastethernet 1"
id="1"
priority="100"
group_id="1"
ip_addr="30.0.0.10"
></data>
<data
name="fastethernet 1"
vlan="100"
id="2"
use_vmac="enabled"
priority="100"
group_id="1"
ip_addr="30.0.0.10"
```

```
></data>
</vrrp>
```

Restoring the system to Factory Default Settings

To delete the current configuration and return the system to its factory defaults, use the following command at the admin prompt.

NOTE: The IP address of interface Management 1, telnet, and the default gateway are left in tact. This done in the event you telneted into the box.

```
[admin@xxxxx bin]$ ./cos_reset_system
```

Getting Help Within the Configuration Tool

To receive help from within the system Configuration Tool, use the following command at the admin prompt.

```
[admin@xxxxx bin]$ ./cos_show_system --help
```

The following options can be used within this Help system:

```
cos_show_system [OPTION...]

-v, --version - displays the current configuration tool
version number.

-h, --help - displays the configuration tool's help
system.

-f, --file=STRING - displays the configuration output
file. The default value is stdout.

-d, --default - tells the Help system to include
default values.
```

5 Upgrading the System Software

This chapter describes how to update your 3COM Security Switch 6200 system software.

Upgrading the System Software

If you are upgrading your system from a previously configured release, you do not need to use the full system software. Instead, you can use the software upgrade patch.

NOTE: "upgradepack-ocode-A*-1.0.0-11-2.1.4-17.shar.gz" is the upgrade pack that will enable you to upgrade from 2.1.x to 2.1.4 (x = 0,1,2). To do this, complete the following:

1. Login to your system Console port as Root.
2. Change to the root directory, using the following command:

   `cd /root`
3. Create a directory, using the following command:

   `mkdir upgradepack-X.X.X-X`

   Where *X.X.X-X*, is the current software version. For this release X sequence is 2.1.4-17
4. FTP or copy the file called cos-upgradepack-ocode-*AZZZ-Y.Y.Y-Y-X.X.X-X*.shar.gz from your system Software CDROM or software package to the /root/upgradepack-*X.X.X-X*.
5. Change the directory to upgradepack-*X.X.X-X*, using the following command:

   `cd upgradepack-X.X.X-X`
6. Enter the following command at the root prompt:

   `gzip –d upgradepack-ocode-AZZZ-Y.Y.Y-Y-X.X.X-X.shar.gz`

7. Once the above command completes, enter the following command at the root prompt:

   `chmod 700 cos-upgradepack-ocode-`*`AZZZ-Y.Y.Y-Y-X.X.X-X`*`.shar`

8. Once the above command completes, enter the following command at the root prompt:

   `./cos-upgradepack-ocode-`*`AZZZ-Y.Y.Y-Y-X.X.X-X`*`.shar`

   Answer "Y" when this command prompts you.

NOTE: Once this action completes successfully, your system software is upgraded.

You may notice "Exec'ed Program Error" being displayed on your screen during the upgrade process if upgrading from a release prior to 2.1.3. Please ignore these error messages. Your system will still be upgraded properly

9. Reboot your system.

6 Upgrading the System Software Using the Safe Upgrade and Rollback Features

Your system ships with two disk partitions, one partition is used for the current runtime (RP) version of software and the other partition is for the upgraded (UP) version of software. Each partition provides 20 Gigabytes of disk space.

This chapter describes how to update your system software, and how to utilize these partitions.

Using Multiple Versions of Software (Safe Upgrade)

Using two partitions, your system allows you to upgrade your system software while maintaining a previous version of your configuration. The following sections describe how to accomplish this.

Upgrading from Version 2.0

To upgrade your system from Version 2.0 to a newer release, while saving your current configuration, complete the following:

1. Connect to Console port as described in the previous section.
2. Partition your disk for dual boot. Note that this only has to be accomplished once. To do this, from root prompt, enter the following command:

   ```
   fdisk /dev/ataraid/d0
   ```

3. Within the fdisk command, display a print(p) disk layout by entering the letter “p”. A display similar to the following displays:

   ```
   /dev/ataraid/d0p1 * 1 13 104422 83 Linux
   ```

   ```
   # /boot
   ```

```
/dev/ataraid/d0p2 14 79 530145 82 Linux swap
/dev/ataraid/d0p5 80 882 6450097 83 Linux # /
/dev/ataraid/d0p6 883 2070 9542609+ 83 Linux

# /opt
/dev/ataraid/d0p7 2071 2435 2931862 83 Linux

# /var
```

4. Duplicate the above table for the dual boot by entering the letter “n” five times. This adds the following partitions:

```
Add(n) the following logical(l) partitions in cylinders

partition    cylinders       partition
8            +12             /boot
9            +65             swap
10           +802            /
11           +1187           /opt
12           +*              /var
```

5. Toggle(t) the swap partition identification from 9 to 82 by entering the letter “t”.
6. Save(w) the partition table by entering the letter “w”.
7. Reboot your system.

You can also perform the software upgrade when you reboot your system using the Install Server. To do this, complete the following:

1. Check to make sure you have the right version of install-cos. To do this:

   At root prompt, enter:

   ```
   /usr/os/sbin/install-cos -h
   ```

   The following displays:

   ```
   Usage: /usr/os/sbin/install-cos [OPTION]... <COS
   RPM DIR>

   Install a C30 release
   h, help
   p <id>, part of disk to install to, 1 or 2
   ```

2. Execute the following command:

   ```
   shell> dd if=/dev/zero of=/dev/ataraid/d0 bsQ2 count=1
   ```

3. Execute the following:

   ```
   /usr/os/bin/install
   ```

4. Reboot and re-run /usr/os/bin/install.

Upgrading from Version 2.1 and Greater

Newer versions of Version 2.1 and greater allow you to do a full copy of the Running Partition (RP) to an Upgrade Partition (UP) before actually upgrading your system software.

To do this:

1. Make sure you are connected to the console.
2. Reboot your system into single user mode. To do this, at the root prompt, enter:

   ```
   init 1
   ```

3. Once the system boots into single user prompt, enter the following:

   ```
   /usr/os/sbin/cos-copy-dist -p 2
   ```

   This copies your entire RP disk contents into the UP. This is a total disk copy and everything on the RP is copied to UP, including the application configurations.

4. Once the copy is complete, enter the following:

   ```
   /usr/os/bin/cos_toggle other
   ```

5. Reboot your system. Your system is booted into the UP.
6. Upgrade your system software or applications, as needed.
7. Reboot if necessary.

If all upgrades are working normally, you are now on the UP (partition set 2). If, however, your upgrades fail, your system fails to boot up, or crashes, then you must reboot and when you get the bootup choices for the kernel under Grub, select the Chains option. Alternatively, if you are able to get to the root prompt but still do not want to upgrade, enter the following:

```
/usr/os/bin/cos_toggle other
```

NOTE: To view the current partition, enter the following:

```
/usr/os/bin/cos_toggle
```

The default value is “/vmlinuz-2.4.18-5” and indicates your original RP.

To list possible selections, enter the following:

```
/usr/os/bin/cos_toggle -l
```

The “other” value indicates the second part of the disk, which is your UP.

Then reboot system.

To go back to the original partition (RP) that was working properly, reboot the system.

Upgrading from Software to a UP While an RP is Operational (Rollback)

Newer versions than 2.1 and greater allow you to install the system software to a UP while an RP is operational. This is done using /usr/os/sbin/install-cos. Install-cos can install to either part 1 or 2 of the disk. You can run install-cos while the system is booted from the install server or the system is running off the disk.

CAUTION:
Caution: Reboot into the UP first, making sure the UP is working, then upgrade within the UP, leaving the good RP alone.

To install to the UP of your system while the system is running with the RP:

1. Enter the following command:

   `/usr/os/sbin/install-cos -p 2 <release directory>`

2. Manually configure the UP identically to the RP (System configuration and applications).
3. Switch to the RP and upgrade the RP.
4. If upgrades work correctly you are done. If, however, the upgrades fail, reboot the system. By default the system boots with the functional UP.

7 Technical Support

3Com provides easy access to technical support information through a variety of services. This chapter describes these services.

Information contained in this chapter is correct at time of publication. For the most recent information, 3Com recommends that you access the 3Com Corporation World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7days a week, through the following online systems:

- World Wide Web site
- 3Com Knowledgebase Web Services
- 3Com FTP site

World Wide Web Site

To access the latest networking information on the 3Com Corporation World Wide Web site, enter this URL into your Internet browser:

http://www.3com.com/

This service provides access to online support information such as technical documentation and software library, as well as support options that range from technical education to maintenance and professional services.

3Com Knowledgebase Web Services

The 3Com Knowledgebase is a database of technical information to help you install, upgrade, configure, or support 3Com products. The Knowledgebase is updated daily with technical information discovered by 3Com technical support engineers. This complimentary service, which is available 24 hours a day, 7 days a week to 3Com customers and partners, is located on the 3Com Corporation World Wide Web site at:

http://www.knowledgebase_3com.com/

3Com FTP Site

Download drivers, patches, software, and MIBs across the Internet from the 3Com public FTP site. This service is available 24 hours a day, 7 days a week.

To connect to the 3Com FTP site, enter the following information into your FTP client:

Hostname: ftp.3com.com

Username: anonymous

Password: <your Internet e-mail address>

Note: You do not need a user name and password with Web browser software such as Netscape Navigator and Internet Explorer.

Support from Your Network Supplier

If you require additional assistance, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to obtain assistance from the 3Com online technical resources or from your network supplier, 3Com offers email and telephone technical support services. To find out more about your support options, email or call the 3Com technical support services at the location nearest you.

Email Support

Some 3Com regions offer an email support service. To access this service for your region, use the appropriate URL or email address from the list below.

Asia, Pacific Rim

From this region, email: apr_technical_support@3com.com

Europe, Middle East and Africa

Enter the URL: http://emea.3com.com/support/email.html

Latin America

Spanish speakers, enter the URL: http://lat.3com.com/lat/support/form.html

Portuguese speakers, enter the URL: http://lat.3com.com/br/support/form.html

English speakers, email: lat_support_anc@3com.com

Telephone Support

When you contact 3Com for assistance, have the following information ready:

- Product model name, part number, and serial number
- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

The following table provides a list of worldwide technical telephone support numbers. These numbers are correct at the time of publication. Refer to the 3Com Web site for updated information.

Telephone Support Numbers

Country	Telephone Number	Country	Telephone Number
Asia, Pacific Rim	1 800 678 515	**Europe, Middle East and Africa**	
	+61 2 9424 5179 or		
Australia	000800 6501111		
India	001 803 61 009	From anywhere in	+44 (0)1442 435529
	1800 801 777	these regions, call:	phone
Indonesia	0800 446 398		
Malaysia	+61 2 9937 5083	Austria	01 7956 7124
New Zealand	1235 61 266 2602 or	Belgium (Flemish)	070 700 000
Pakistan	+61 2 9937 5076	Belgium (French)	070 700 770
Philippines	800 6161 463	Denmark	7010 7289
	00798 611 2230 or	Finland	01080 2783
Singapore	02 3455 6455	France	0825 809 622
S. Korea	0080 611 261	Germany	01805 404 747
	001 800 611 2000	Hungary	06800 14466
Taiwan		Ireland	1800 509359
Thailand		Israel	1800 943 2632
		Italy	199 161346
		Luxembourg	800 29880
		Netherlands	0900 777 7737
		Norway	815 33 047
		Poland	00800 441 1357
		Portugal	707 200 123
		South Africa	0800 991196
		Spain	9 021 60455
		Sweden	07711 14453
		Switzerland	08488 50112
		U.K.	0870 241 3901

Country	Telephone Number	Country	Telephone Number
Latin America		**North America**	1 800 876 3266
From the Caribbean,	1 800 988 2112		
Central and South	0 810 444 3COM		
America, call:	1 800 998 2112		
Antigua	1 800 998 2112		
Argentina	1 800 998 2112		
Aruba	52 5 201 0010		
Bahamas	1 800 998 2112		
Barbados	1 800 998 2112		
Belize	0800 13 3COM		
Bermuda	1 800 998 2112		
Bonaire	AT&T +800 998		
Brazil	112		
Cayman	AT&T +800 998		
Chile	2112		
Colombia	AT&T +800 998		
Costa Rica	2112		
Curacao	1 800 998 2112		
Ecuador	AT&T +800 998		
Dominican Republic	2112		
Guatemala	AT&T +800 998		
Haiti	2112		
Honduras	AT&T +800 998		
Jamiaca	2112		
Martinique	57 1 657 0888		
Mexico	AT&T +800 998		
Nicaragua	2112		
Panama	1 800 998 2112		
Paraguay	571 657 0888		
Peru	01 800 849CARE		
Puerto Rico	AT&T +800 998		
Salvador	2112		
Trinidad and Tobago	AT&T +800 998		
Uruguay	2112		
Venezuela	54 11 4894 1888		
Virgin Islands	AT&T +800 998		
	2112		
	1 800 998 2112		
	AT&T +800 998		
	2112		
	1 800 998 2112		
	AT&T +800 998		
	2112		
	AT&T +800 998		
	2112		
	57 1 657 0888		

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain an authorization number. Products sent to 3Com without authorization numbers will be returned to the sender unopened, at the sender's expense.

You can obtain an authorization number (called an RMA) by entering the following URL into your Internet browser:

http://www.3com.com/support/en_US/repair

Alternatively, you can obtain an RMA by calling or faxing one of the numbers in the following table:

Fax Numbers for return authorization numbers

Country	Telephone Number	Fax Number
Asia, Pacific Rim	+65 543 6500	+65 543 6348
Europe, Middle East and Africa Austria Belgium (Flemish) Belgium (French) Denmark Finland France Germany Hungary Ireland Israel Italy Luxembourg Netherlands Norway Poland Portugal South Africa Spain Sweden Switzerland U.K.	+44 (0)1442 435529 01 7956 7124 070 700 000 070 700 770 7010 7289 01080 2783 0825 809 622 01805 404 747 06800 14466 1800 509359 1800 943 2632 199 161346 800 29880 0900 777 7737 815 33 047 00800 441 1357 707 200 123 0800 991196 9 021 60455 07711 14453 08488 50112 0870 241 3901	
USA and Canada	1 800 876 3266	1 508 323 6061 (not toll free)

Country	Telephone Number	Fax Number
Latin America		
Antigua	1-800-988-2112	
Argentina	0-810-444-3COM	
Aruba	1-800-998-2112	
Bahamas	1-800-998-2112	
Barbados	1-800-998-2112	
Belize	52-5-201-0010	
Bermuda	1-800-998-2112	
Bonaire	1-800-998-2112	
Brazil	0800-13-3COM	
Cayman	1-800-998-2112	
Chile	AT&T +800-998-2112	
Colombia	AT&T +800-998-2112	
Costa Rica	AT&T +800-998-2112	
Curacao	1-800-998-2112	
Ecuador	AT&T +800-998-2112	
Dominican Republic	AT&T +800-998-2112	
Guatemala	AT&T +800-998-2112	
Haiti	57-1-657-0888	
Honduras	AT&T +800-998-2112	
Jamiaca	1-800-998-2112	
Martinique	57-1-657-0888	
Mexico	01-800-849CARE	
Nicaragua	AT&T +800-998-2112	
Panama	AT&T +800-998-2112	
Paraguay	54-11-4894-1888	
Peru	AT&T +800-998-2112	
Puerto Rico	1-800-998-2112	
Salvador	AT&T +800-998-2112	
Trinidad and Tobago	1-800-998-2112	
Uruguay	AT&T +800-998-2112	
Venezuela	AT&T +800-998-2112	
Virgin Islands	57-1-657-0888	

Technical Specifications

A

This appendix lists the physical, environmental, and power characteristics of the 3COM Security Switch 6200.

Physical Characteristics

Size (Inches): 3.5 H x 17.5 W x 25.5 D
Weight: approximately 32 lbs

Environmental Characteristics

Operating Temperature: 0 to +40 degrees C
Storage Temperature: -20 to +65 degrees C
Relative Humidity: 10 to 95 percent, non-conducting
Operating Altitude: 0 to 10,000 feet above sea level

Power Characteristics

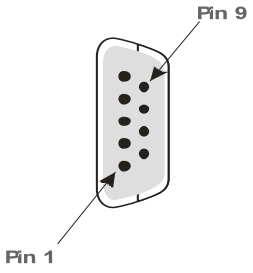
Power: 100 to 240 VAC, 350W

Connector Pin Assignments

B

This appendix describes the craft port pin assignments:

The Craft port, located on the front of the system, uses a DB- 9 connector with the following pin identifications and associated signals.

DB-9 Connector	Pin Number	Signal
	1	No Connection
	2	TDX
	3	RXD
	4	DSR
	5	GND
	6	DTR
	7	CTS
	8	RTS
	9	No Connection

Regulatory Information

C

This appendix provides the following compliance statements:

- Regulatory Standards Compliance
- Radio Frequency Interference
- VCCI Statement

Regulatory Standards Compliance

The following regulatory agencies have approved the 3COM Security Switch 6200 and have found it to be fully compliant with their environmental, safety, and emissions standards.

CE marking for the EEA (European Economic Area)

- Low Voltage Directive 73/23/EEC
- EMC Directive 89/336/EEC

Safety

- IEC 60950
- UL 60950
- CSA C22.2 No. 60950

Factory Approvals

- UL/CSA

EMI Compliance

Radio Frequency Interference

NOTE

In accordance with FCC Part 15 Subpart B requirements, changes or modifications made to this equipment not expressly approved by 3COM Corporation could void the user's authority to operate this equipment.

The 3COM Security Switch 6200 is designed for Class A use only. Do not attempt to use this equipment in a domestic environment, which requires Class B distinction. The system may cause interference with domestic products.

This equipment produces electromagnetic energy at radio frequencies and, if not installed and operated in accordance with 3COM instructions, as contained in this document, could cause interference to radio communications and/or interfere with the operation of other RF devices. This equipment has been tested and found to comply with the limits for a Class A Computing Device pursuant to Subpart B of Part 15 of the FCC Rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area may cause interference. Should this occur, the user may be required to discontinue operation of the equipment, or take other such measures as may be adequate to rectify the condition at the user's expense.

VCCI Statement V-3/2000.04

This is a Class A product based on the standards of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Other EMI Approvals

- EN 55022
- AS/NZS 3548:95
- BSMI CNS 13438 Class A

Immunity Compliance

The system meets all EN 55024 immunity testing.